UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/289,513	04/09/1999	PHILIP R. WISER	P-2090	8705

7590 12/17/2003

EXAMINER
GILLIGAN, CHRISTOPHER L

ART UNIT	PAPER NUMBER
3626	

Steven J Rocci
Woodcock Washburn LLP
One Liberty Place
46th Floor
Philadelphia, PA 19103

DATE MAILED: 12/17/2003

25

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS
UNITED STATES PATENT AND TRADEMARK OFFICE
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Paper No. 25

Application Number: 09/289,513
Filing Date: April 09, 1999
Appellant(s): WISER ET AL.

Kenneth R. Eiferman
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 17 September 2003.

(1) Real Party in Interest

A statement identifying the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

A statement identifying the related appeals and interferences which will directly affect or be directly affected by or have a bearing on the decision in the pending appeal is contained in the brief.

(3) Status of Claims

The statement of the status of the claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Invention

The summary of invention contained in the brief is correct.

(6) Issues

The appellant's statement of the issues in the brief is correct.

(7) Grouping of Claims

Appellant's brief includes a statement that claims 1-49 do not stand or fall together and provides reasons as set forth in 37 CFR 1.192(c)(7) and (c)(8).

(8) Claims Appealed

The copy of the appealed claims contained in the Appendix to the brief is correct.

(9) Prior Art of Record

5,715,314	Payne et al.	02-1998
6,236,971	Stefik et al.	05-2001

(10) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

Claims 1-3, 10-26, and 39-49 are rejected under 35 U.S.C. 102(e) as being anticipated by Payne et al., U.S. Patent No. 5,715,314.

As per claim 1, Payne et al. teach a method for conducting electronic commerce through a computer network, the method comprising: receiving, in a merchant computer system of the computer network, a purchase request for a digital product (see column 5, lines 26-29, payment computer of Payne et al. is read upon by the merchant system); receiving payment data in the merchant computer system wherein the payment data specifies remuneration for the digital product (see column 5, lines 29-34, this step is preformed by the payment computer of Payne et al.); sending a request for reservation of the digital product to a content manager computer system which can be different from the merchant computer system and which is coupled to the merchant computer system through the computer network (see column 7, lines 31-33, merchant computer of Payne et al. is read upon by the content manager, the request includes a request to reserve access to the digital document for a specified duration of time; the two computers are coupled via network 10 of Payne et al, see figure 1); receiving, in the content manager computer system a delivery request signal from the merchant computer system wherein the delivery request signal requests delivery of the digital product to a client computer system through the computer network (see column 7, lines 31-39, the delivery request is sent from the payment computer to the merchant computer via the buyer computer); sending transaction identification data to the client computer system wherein the transaction identification data identifies the

digital product and represents remuneration in accordance with the payment data (see column 7, lines 18-24 and lines 31-32); receiving, in a delivery computer system of the computer network, the transaction identification data from the client computer system (see column 7, lines 32-33); determining within the delivery computer system, in accordance with the transaction identification data, the digital product (see column 7, lines 27-33); and sending, from the delivery computer system, the digital product to the client computer system (see column 7, lines 46-50).

As per claim 2, Payne et al. teach the method of claim 1 as described above, further comprising: sending, from the delivery computer system to the content manager computer system, a signal indicating that sending the digital product to the client computer system is completed (see column 3, lines 24-27).

As per claim 3, Payne et al. teach the method of claim 2 as described above, further comprising: recording, by the content manager computer system, purchase data identifying the digital product and indicating that the digital product was purchased (see column 3, lines 24-27).

As per claim 10, Payne et al. teach the method of claim 1 as described above, wherein requesting reservation by the merchant computer system comprises: encrypting data representing a requested reservation (see column 1, lines 59-64); sending the data as encrypted to the content manager computer system (see column 1, line 64 – column 2, line 2); and decrypting the data within the content manager computer system (see column 1, line 64 – column 2, line 2, the data has to be decrypted to be viewed).

As per claim 11, Payne et al. teach the method of claim 1 as described above, wherein, in response to requesting reservation by the merchant computer system, the content manager computer system effects such a reservation of the digital product by: forming transaction data which include (i) the transaction identification data, (ii) product identification data which identifies the digital product, and (iii) binding data which binds the transaction to the client computer

system (see column 5, lines 30-44); and sending the transaction data to the merchant computer system (see column 5, lines 48-53).

As per claim 12, Payne et al. teach the method of claim 11 as described above, wherein sending the transaction identification data comprises encrypting the transaction identification data (see column 5, lines 42-47).

As per claim 13, Payne et al. teach the method of claim 1 as described above, further comprising: sending, from the merchant computer system, the payment data to a payment authority (see column 1, lines 55-59); and receiving, in the merchant computer system from the payment authority, payment authorization data (see column 1, lines 59-64).

As per claim 14, Payne et al. teach the method of claim 13 as described above, further comprising: sending the payment authorization data to the content manager computer system (see column 2, lines 11-18).

As per claim 15, Payne et al. teach the method of claim 14 as described above, wherein sending the payment authorization data comprises: encrypting the payment authorization data (see column 1, line 64 – column, line 2).

As per claim 16, Payne et al. teach the method of claim 14 as described above, further comprising recording, by the content manager computer system, that payment for the digital product has been authorized (see column 2, lines 3-11).

As per claim 17, Payne et al. teach the method of claim 16 as described above, further comprising: receiving, in the merchant computer system from the content manager computer system, acknowledgment data which indicates that payment for the digital product has been recorded (see column 2, lines 11-18).

As per claim 18, Payne et al. teach the method of claim 17 as described above, wherein acknowledgement data includes the transaction identification data and a payment authorization

token which identifies payment authorization as recorded by the content manager computer system (see column 2, lines 11-18).

As per claim 19, Payne et al. teach the method of claim 18 as described above, wherein the delivery request signal includes the transaction identification data and the delivery authorization token (see column 6, lines 30-41).

As per claim 20, Payne et al. teach the method of claim 19 as described above, wherein the delivery request signal is generated in response to selection of a URL by the user wherein the URL specifies the transaction identification data and the delivery authorization token (see column 6, lines 31-35).

As per claim 21, Payne et al. teach the method of claim 17 as described above, wherein the acknowledgement data is encrypted (see column 1, line 64 – column 2, line 2).

As per claim 22, Payne et al. teach the method of claim 1 as described above, wherein the delivery request signal is received in the content manager computer system from the client computer system (see column 4, lines 60-63); and further wherein the delivery request signal is generated by the client computer system in response to user-generated control signals (see column 4, lines 35-37).

As per claim 23, Payne et al. teach the method of claim 22 as described above, wherein the user-generated control signals are incident to a graphical user interface of a web browser (see column 4, lines 43-45 and figure 5); and further wherein the user-generated control signals cause the client computer system to send the delivery request signal to the merchant computer system which in turn communicates the delivery request signal to the content manager computer system (see column 4, lines 60-63).

As per claim 24, Payne et al. teach the method of claim 1 as described above, wherein the delivery request signal includes the transaction identification data (see column 5, lines 27-44).

As per claim 25, Payne et al. teach the method of claim 24 as described above, wherein the delivery request signal is generated in response to selection of a URL by the user wherein the URL specifies the transaction identification data (see column 5, lines 27-30).

As per claim 26, Payne et al. teach the method of claim 1 as described above, wherein the transaction identification data, as received by the delivery computer system is certified as originating from the client computer system (see column 5, line 42, particularly the "buyer network address").

As per claim 39, Payne et al. teach a method for conducting electronic commerce through a computer network, the method comprising: receiving, in a merchant computer system of the computer network, a purchase request for a digital product (see column 5, lines 26-29, payment computer of Payne et al. is read upon by the merchant system); receiving payment data in the merchant computer system wherein the payment data specifies remuneration for the digital product (see column 5, lines 29-34, this step is preformed by the payment computer of Payne et al.); sending a request for reservation of the digital product to a content manager computer system which can be different from the merchant computer system and which is coupled to the merchant computer system through the computer network (see column 7, lines 31-33, merchant computer of Payne et al. is read upon by the content manager, the request includes a request to reserve access to the digital document for a specified duration of time; the two computers are coupled via network 10 of Payne et al, see figure 1); receiving, from the content manager computer system, voucher data which is readable by the content manager computer system and which represents to the content manager computer system a transaction

in which the remuneration specified by the payment data is exchanged for the digital product (see column 5, lines 48-56).

As per claim 40, Payne et al. teach the method of claim 39 as described above, further comprising: receiving, from the content manager computer system, inventory data which specifies available digital products, including the digital product, and specified remuneration to the content manager computer system for each of the available digital products (see column 4, lines 46-49).

As per claim 41, Payne et al. teach the method of claim 40 as described above, wherein requesting reservation comprises: encrypting data representing a requested reservation (see column 1, lines 59-64); sending the data as encrypted to the content manager computer system (see column 1, line 64 – column 2, line 2); and decrypting the data within the content manager computer system (see column 1, line 64 – column 2, line 2, the data has to be decrypted to be viewed).

As per claim 42, Payne et al. teach the method of claim 40 as described above, further comprising: sending, from the merchant computer system, the payment data to a payment authority (see column 1, lines 55-59); and receiving, in the merchant computer system from the payment authority, payment authorization data (see column 1, lines 59-64).

As per claim 43, Payne et al. teach the method of claim 42 as described above, further comprising: sending the payment authorization data to the content manager computer system (see column 2, lines 11-18).

As per claim 44, Payne et al. teach the method of claim 43 as described above, wherein sending the payment authorization data comprises: encrypting the payment authorization data (see column 1, line 64 – column, line 2).

As per claim 45, Payne et al. teach the method of claim 44 as described above, further comprising: receiving, in the merchant computer system from the content manager computer system, acknowledgment data which indicates that payment for the digital product has been recorded (see column 2, lines 11-18).

As per claim 46, Payne et al. teach the method of claim 45 as described above, wherein acknowledgement data includes the transaction identification data and a payment authorization token which identifies payment authorization as recorded by the content manager computer system (see column 2, lines 11-18).

As per claim 47, Payne et al. teach the method of claim 46 as described above, wherein the delivery request signal includes the transaction identification data and the delivery authorization token (see column 6, lines 30-41).

As per claim 48, Payne et al. teach the method of claim 47 as described above, wherein the delivery request signal is generated in response to selection of a URL by the user wherein the URL specifies the transaction identification data and the delivery authorization token (see column 6, lines 31-35).

As per claim 49, Payne et al. teach the method of claim 45 as described above, wherein the acknowledgement data is encrypted (see column 1, line 64 – column 2, line 2).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 4-9, and 27-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Payne et al., U.S. Patent No. 5,5715,314 in view of Stefik et al., U.S. Patent No. 6,236,971.

As per claim 4, Payne et al. teach the method of claim 3 as described above. Payne et al. do not explicitly teach apportioning compensation for sales of the digital product through a media licensing computer system. Stefik et al. teach apportioning compensation for sales of the digital product through a media licensing computer system (see column 4, lines 40-48). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the licensing capabilities of Stefik et al. with the electronic commerce environment of Payne et al. One of ordinary skill in the art would have been motivated to include this element for the purpose of provide a more diverse purchasing option to a prospective buyer.

As per claim 5, Payne et al. in view of Stefik et al. teach the method of claim 4 as described above, further comprising: aggregating purchase data from the content manager computer system and other purchase data from one or more other content manager computer system to form aggregated purchase data (see column 7, lines 55-59); and sending the aggregated purchase data to a rights agent computer system such that the rights agent computer system can apportion compensation for sales of the digital product (see column 7, lines 59-65).

As per claim 6, Payne et al. in view of Stefik et al. teach the method of claim 5 as described above. Payne et al. do not explicitly teach encrypting the purchase data in such a manner that data held secret by the media licensing computer system is required for decrypting the purchase data. Stefik et al. teach encrypting data in such a manner that data held secret by the media licensing computer system is required for decrypting the data (see column 26, lines 58-63). It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this encryption feature into the system of Payne et al. One of ordinary skill in the

art would have been motivated to make such a modification for the purpose of enhancing the security of data communications within the system of Payne et al.

As per claim 7, Payne et al. in view of Stefik et al. teach the method of claim 6 as described above. Payne et al. do not explicitly teach encrypting the purchase data in such a manner that modifications of the purchase data subsequent to the encrypting can be detected. Stefik et al. teach encrypting data in such a manner that modifications of the data subsequent to the encrypting can be detected (see column 12, lines 50-57). It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate such a security measure into the system of Payne et al. One of ordinary skill in the art would have been motivated to incorporate such a feature for the purpose of enhancing security of stored data.

As per claim 8, Payne et al. in view of Stefik et al. teach the method of claim 6 as described above. Payne et al. do not explicitly teach encrypting the purchase data in such a manner that removal of the purchase data from a sequence of purchase data records subsequent to the encrypting can be detected. Stefik et al. teach encrypting data in such a manner that removal of the data from a sequence of data records subsequent to the encrypting can be detected (see column 12, lines 50-57). It would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate such a security measure into the system of Payne et al. One of ordinary skill in the art would have been motivated to incorporate such a feature for the purpose of enhancing security of stored data.

As per claim 9, Payne et al. teach the method of claim 1 as described above. Payne et al. do not explicitly teach encrypting the digital product before sending it to the client computer system and then decrypting it once in the client computer system. Stefik et al. teach encrypting the digital product before sending it to the client computer system and then decrypting it once in the client computer system (see column 26, lines 39-52, column 37, lines 40-43 and lines 57-

62). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the encrypting element of Sefik et al. with the electronic commerce method of Payne et al. for the purpose of providing increased security to users of the system.

Claims 27-38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Payne et al., U.S. Patent No. 5,715,314. Payne et al. teach the method of claim 26 as described above. Payne et al. do not explicitly teach the specific types of digital products in claims 27-38. However, these types of digital media were old and well known at the time the invention was made. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include any of these types of digital media in the method of Payne et al. for the purpose of providing a more diverse selection to buyers.

(11) Response to Argument

In the Appeal Brief filed 17 September 2003, Appellants make the following arguments:

A) Payne fails to teach a system in which the same computer system both receives a purchaser's payment for a product, and sends a request to another system directing that the purchaser receive the product.

B) The buyer computer does not act as a mere conduit for transmitting the "access URL" from the payment computer to the merchant computer.

C) Payne does not teach that the payment computer and merchant computer are "coupled" to each other through a computer network.

D) Neither Payne nor Stefik teach discarding of an encryption key.

E) Payne does not teach an additional "payment authority" separate from the payment computer, merchant computer, and buyer computer.

Examiner will address Appellant's arguments in sequence as they appear in the

Brief.

Response to argument A:

In response to the first argument, it is first noted by the Examiner that none of the limitations recited in claim 1 require a payment to be received in any computer system. Rather, the second step requires that "payment data" which "specifies remuneration for the digital product" be received in the merchant computer system (payment computer of Payne). The Examiner interprets the "payment amount" which is part of "payment URL A" sent to the payment computer to be a form of "payment data" which specifies remuneration for the digital product" (see column 5, lines 30-35). Furthermore, the same payment computer of Payne sends an "access URL" which includes a product identifier and an indication of how long access to the product should be granted, among other information. The Examiner interprets this information sent by the payment computer of Payne to be a form of sending a request that the purchaser receive the product. Therefore, the Examiner respectfully submits that Payne does in fact teach a single computer system that both receives a purchaser's payment data for a product, and sends a request to another system directing that the purchaser receive the product.

Response to argument B:

In response to the second argument, the Examiner respectfully disagrees with Appellants' interpretation of the teachings of Payne for several reasons. First, Appellants assert that the "access URL" of Payne is sent from the payment computer to the buyer computer, the buyer computer "processes that data in some way", and then sends different data on to the merchant computer (see Appeal Brief, page 9). In support of this assertion, Appellants cite column 9, lines 51-61 of Payne, however, neither this passage nor any other teachings of Payne

support this interpretation. In fact, the cited portion of Payne merely states that unless a URL is specified as a redirection, all URLs are transmitted between computers in a standard HTTP request message. It should be noted that this passage says nothing with regard to receiving one set of data, "processing it in some way," and sending different data on to another computer. It should also be noted that the portion of Payne that describes the transmission of the "access URL" to the buyer computer, and then to the merchant computer is likewise devoid of any suggestion that the buyer computer "processes that data in some way" before sending it on to the merchant computer (see column 7, lines 15-50, with particular emphasis on lines 31-33).

In addition, the "access URL" created by the payment computer contains six important pieces of information which much be sent to the merchant computer so that the merchant computer can carry out the proper verification steps before giving the buyer computer access to the product (see column 7, lines 34-54 and Figure 2G extending to 2H). It is important to note that the merchant computer must verify that the "access URL authenticator" was created from the contents of the "access URL" using the cryptographic key, verify that the duration time indicated in the "access URL" has not expired, and verify that the buyer computer network address is the same as the buyer network address in the "access URL." Therefore, even if Appellants' assertion that the buyer computer "processes the data in some way" to send different data to the merchant computer, which the Examiner finds no reason to be the case, the important information, which represents the delivery request signal, sent by the payment computer must be the same information received by the merchant computer for the system of Payne to function properly.

Finally, the Examiner wishes to note that in the summary of the Invention Payne describes the process of sending the access message to the merchant computer as follows at column 1, line 59 – column 2, line 2:

> The payment computer is programmed to receive the payment message, to cause an access message to be created that comprises the product identifier and an access message authenticator based on a cryptographic key, and to cause the access message to be sent to the merchant computer. The merchant computer is programmed to receive the access message, to verify the access message authenticator to ensure that the access message authenticator was created using the cryptographic key, and to cause the product to be sent to the user desiring to buy the product.

In this passage, Payne describes the process of communicating the access message between the payment computer and the merchant computer without any mention of the buyer computer. Therefore, the Examiner respectfully submits that the interpretation of Payne as applied in the rejections is proper.

Response to Argument C:

In response to the third argument, the Examiner respectfully submits that Figure 1 of Payne clearly displays a system in which each computer (buyer, payment, merchant, and creation) are "coupled" to one another through network 10. In addition, Payne explicitly states that the "buyer, merchant, payment, and creation computers are all inter-connected by a computer network 10 such as the Internet." (see column 4, lines 43-45). Therefore, the Examiner fails to understand how Appellants can assert that the payment computer and merchant computer are not "coupled" to each other through a computer network.

Response to Argument D:

In response to the fourth argument, the Examiner respectfully submits that the use of a "one-time" key as taught by Stefik has been relied upon to teach this limitation. In particular, Stefik teaches the process of encrypting a digital work using the "one-time" key and discarding it to a "restoration file." (see column 37, lines 40-43). Clearly, this key is only intended to be used once unless a catastrophic media failure occurs (see column 37, lines 57-62). It should also be noted that the terms "discarding" and "intended to be used only once" with respect to the key

have been given the broadest reasonable interpretation to one of ordinary skill in the art of encryption. In this case, the Examiner has interpreted these terms to encompass permanently storing the key in a location after it has been used once and only retrieving it under unusual circumstances not "intended" to occur.

Response to Argument E:

In response to the final argument, the Examiner respectfully submits that the claims do not require an additional party, other than the described computer systems, to represent the "payment authority." In particular, the claims merely recite that payment data is sent to "a payment authority" and that payment authorization data is received from the "payment authority." Therefore the Examiner respectfully submits that the computer systems taught by Payne clearly meet these steps required to be performed by "a payment authority" as detailed above in the rejections.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Christopher Gilligan
Assistant Patent Examiner
Tech Center 3600

CLG
December 12, 2003

Conferees

Joseph Thomas J.T.
Supervisory Patent Examiner
Tech Center 3600

James Trammell
Supervisory Patent Examiner
Tech Center 3600

JOSEPH THOMAS
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600

STEVEN J ROCCI
WOODCOCK WASHBURN LLP
ONE LIBERTY PLACE
46TH FLOOR
PHILADELPHIA PA 19103